JOURNAL OF NUMBER THEORY 8, 308–312 (1976)

On the Invertibility of Ideals in Orders

DANIEL FALK

R.F.D. 1, Marshfield, Vermont 05658

Communicated by H. Zassenhaus

Received September 1, 1972

The problem of invertibility of ideals in orders has been studied by a number of authors. The commutative case has been considered by Dade, Taussky, and Zassenhaus; Frolich; and Singer. Ballew gives a generalization of Frolich's results to a class of noncommutative orders. We examine some of the possible extensions of the results of Dade *et al.* to noncommutative orders.

1

We begin by stating the main theorems of [2] in somewhat less generality than they were proved.

THEOREM 1. *Let M be a finitely generated Z module in the number field K. Then:*

(a) *M^t is invertible for all integers $t \geqslant t_0$. (By M^t we mean the module formed by all sums of the form: $\sum m_1 m_2 \cdots m_t$, $m_i \in M$.)*

(b) *t_0 can be chosen less than $|K : Q|$.*

By invertible here we mean that there is a finitely generated Z module N such that $MN = O(M)$, where $O(M)$ is the order of M or its multiplier domain in K.

For the noncommutative case we need some further definitions and notation. Let

$R =$ Dedekind domain with finite residue class fields at all primes.

$K =$ quotient field of R.

$A =$ central simple K-algebra.

$M =$ finitely generated R module in A such that $K \cdot M = A$. (M is called an ideal or by some authors, a full R module.)

$L(M)$, $(R(M)) =$ left (right) order of M.

DEFINITION 1. $\overline{M} = \{x \mid x \in A \text{ and } MxM \subset M\}$.

DEFINITION 2. [3] M is weakly invertible if $M\overline{M}M = M$.

DEFINITION 3. M is left (right) invertible if $M\overline{M} = L(M)$ ($\overline{M}M = R(M)$).

DEFINITION 4. M is two-sided invertible if it is both left and right invertible.

DEFINITION 5. M is two-sided O invertible if is two-sided invertible and $L(M) = R(M) = O$.

First, some remarks about the definitions. It is clear that 5 implies 4, 4 implies 3, 3 implies 2. Also, 2–5 coincide for commutative orders. We also remark that there are modules M which are right invertible and not left invertible (see Sect. 2) and modules which are two-sided invertible but not two-sided O invertible, i.e., any module whose left and right orders are maximal but not equal.

Of the following generalizations of part (a) of Theorem 1, only (2.4) is true.

THEOREM 2. *Let M be an ideal in A. Then some power of M is*

(2.1) *two-sided O invertible,*

(2.2) *two-sided invertible,*

(2.3) *left or right invertible,*

(2.4) *weakly invertible.*

A counterexample to (2.1), (2.2), and (2.3) is given in Section 2. It is an idempotent module which has none of the properties (2.1)–(2.3). For Theorem 1, part (b) we might consider the following generalizations.

THEOREM 3. *Let M be an ideal in A. Let t be the smallest integer such that M^t is*

(3.1) *two-sided O invertible;*

(3.2) *two-sided invertible;*

(3.3) *left or right invertible;*

(3.4) *weakly invertible. (We let $t = 0$ if no power of M has the property.) Then $t < |A : K|$.*

Of these (3.3) and (3.4) are known to be false, (see Section 2). There is some evidence that (3.1) is true but it is as yet unproved.

The proof of Theorem 2.4 turns on the following lemma for orders over R_P, the localization of R at a prime ideal P of R.

LEMMA 1. *Let O be an R_P order in A. Let M be a two-sided O ideal $(O \subset L(M) \cap R(M))$. Further, suppose that $M \subset O$ and $M \not\subset PO$. Then there is an integer $s \geqslant 1$ such that $M \supset P^sO$. The integer s is independent of M but dependent on the order O.*

Proof. Let O' be a maximal R_P order containing O. It is well known, (see [5]), that O' has a unique maximal two-sided ideal $\bigwedge$, and that all two-sided O' ideals are powers of $\bigwedge$. Hence the ideal $M' = O'MO'$ is a power of $\bigwedge$, say $\bigwedge^d$. Further, it is clear that some power of $\bigwedge$, say $\bigwedge^e$, is contained in PO. This is true since DO' is contained in O where D is the discriminant of O and since PO' is a two-sided O' ideal it is $\bigwedge^j$ for some j. Hence $D\bigwedge^j$ is again a power of $\bigwedge$ and this we will take as $\bigwedge^e$. It is easily seen that $\bigwedge^e \subset \bigwedge^d$, for if not then

$PO \supset \bigwedge^e \supseteq \bigwedge^d = O'MO' \supset M$, a contradiction. We now claim that

$$\begin{aligned}\bigwedge^{3e} \subset M.\ \bigwedge^{3e} = \bigwedge^e\bigwedge^e\bigwedge^e \subset \bigwedge^e\bigwedge^d\bigwedge^e &= \bigwedge^eO'MO'\bigwedge^e \\ &= \bigwedge^eM\bigwedge^e \\ &\subset POMPO \\ &= P^2M \\ &\subset M.\end{aligned}$$

But, since $\bigwedge$ and O are both R_P modules of the same R_P rank, there is some power of P, say P^s, such that $P^sO \subset \bigwedge^{3e}$, hence $P^sO \subset M$. Q.E.D.

We can now define a local equivalence relation on O ideals M by $M \sim N$ iff $M = P^jN$ for some integer j. If $[M] = \{N \mid N \sim M\}$, we can define $[M_1] \cdot [M_2] = [M_1M_2]$. It is easily checked that this operation is well defined and hence gives a semigroup structure to the equivalence classes. If we consider only powers of a fixed class $[M]$, we have abelian semigroup. By virtue of Lemma 1 we can choose a representative for each power of M lying between $O = L(M) \cap R(M)$ and P^sO for some integer s. Since R/P is finite and A is a finite-dimensional K algebra, we have that O/P^sO is also finite. Therefore, the powers of $[M]$ form a finite abelian semigroup, and hence contain an idempotent class. It follows easily that an idempotent class contains a (unique) idempotent ideal, for if $M^{2t} = P^kM^t$, then the ideal $P^{-k}M^t$ is idempotent. Therefore we have proved:

LEMMA 2. *Let M be a finitely generated R_P module in A such that $K \cdot M = A$. Then some power of M is of the form P^tI, where I is an idempotent R_P module.*

From Definition 1, we see that $M\overline{M}M \subset M$ for all M; hence idempotent ideals are weakly invertible, for $\overline{M}$ clearly contains M in this case. If we now return to the situation where R is an arbitrary Dedekind domain, through localization we may simply apply Lemma 2 to show that for each prime P of R there is an integer t_P such that M_P (the localization of M at P) raised to the t_P power is weakly invertible. We now note that for all but a finite number of primes of R, $O = L(M) \cap R(M)$ localizes to a maximal R_P order, and therefore all of its two-sided ideals are two-sided invertible. For these primes, we take $t_P = 1$. If we let $\hat{t} = \prod t_P$ we see that $(M^{\hat{t}})_P$ is weakly invertible for all P. Since local weak invertibility implies global weak invertibility (see [3, p. 187],) we have now proved Theorem 2.4.

In fact, a somewhat stronger statement holds. By examining the right and left inertial ideals of powers of M ([3, p. 181]) we can show that for all $t > \hat{t}$, M^t is weakly invertible.

2

In this section we give a few examples to show some of the difficulties that arise in ideals of a very simple structure. We consider ideals M in $A = K^{n\times n}$. We further assume that $L(M) \cap R(M)$ contains n orthogonal idempotent elements. Hence, by a proper choice of basis, M may be written as a matrix each of whose entries is an ideal of R. If we restrict ourselves further and assume that each of these ideals of R is a power of a fixed ideal of R, then M may be written as a matrix of integers, each representing the power of this fixed ideal. Further, any matrix of integers may be interpreted as an ideal M of this type. Using the formulas of [3], computations can be easily programmed.

EXAMPLE 1. The following ideal is right invertible but not left invertible.

$$M = \begin{pmatrix} 68762 & 49879 & 111996 \\ 82446 & 590 & 62707 \\ 106198 & 69486 & 131603 \end{pmatrix}.$$

A simple calculation gives that

$$\overline{M} = \begin{pmatrix} -68762 & -19483 & -88369 \\ 13094 & -590 & -24342 \\ -49023 & -62707 & -86459 \end{pmatrix}.$$

It is easy to see that $\overline{M}M$ contains three idempotents and hence it is the right order of M. But, $M\overline{M}$ contains only two idempotents.

EXAMPLE 2. The following ideal M is neither left nor right invertible and, since it is idempotent, neither are any of its powers.

$$M = \begin{pmatrix} 0 & a & 2a \\ a & 2a & a \\ 2a & a & 0 \end{pmatrix} \quad \text{for any integer } a.$$

In this case we have

$$\overline{M} = L(M) = R(M) = \begin{pmatrix} 0 & a & 2a \\ a & 0 & a \\ 2a & a & 0 \end{pmatrix}.$$

EXAMPLE 3. The following ideal M is a counterexample to Theorem 3.3 and 3.4. The first power of M which is weakly invertible is 276.

$$M = \begin{pmatrix} 1023 & 5042 & 1042 & 873 & 5858 \\ 7287 & 994 & 383 & 3347 & 6633 \\ 9672 & 8334 & 2956 & 2730 & 9775 \\ 4077 & 6490 & 2242 & 5045 & 89 \\ 5127 & 9956 & 3593 & 1947 & 9348 \end{pmatrix}.$$

In this case we have that the 276th power of M is also right invertible. Hence this is a counterexample to both conjectures.

REFERENCES

1. D. BALLEW, The module index and invertible ideals, *Trans. Amer. Math. Soc.* **148** (1970), 171–184.
2. E. C. DADE, O. TAUSSKY AND H. ZASSENHAUS, On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field, *Math. Ann.* **148** (1962), 31–64.
3. D. K. FADDEEV, Introduction to the multiplicative theory of modules of integral representations, *Proc. Steklov Inst. Math.* **80** (1965), 145–182.
4. A. FROLICH, Invariants for modules over commutative seperable orders, *Quart. J. Math. Oxford Ser. 2* **16** (1965), 193–232.
5. K. ROGGENKAMP AND V. HUBER-DYSON, Lattices over orders, I, Lecture Notes in Mathematics, No. 115, Springer-Verlag, Berlin/New York, 1970.